(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: **0 583 709 A1**

(12) EUROPEAN PATENT APPLICATION

(21) Application number: **93112678.3**

(51) Int. Cl.[5]: **G06K 19/10, G07F 7/08**

(22) Date of filing: **07.08.93**

(30) Priority: **17.08.92 EP 92402297**

(43) Date of publication of application:
23.02.94 Bulletin 94/08

(84) Designated Contracting States:
DE ES FR GB IT

(71) Applicant: **THOMSON CONSUMER ELECTRONICS S.A.**
9, Place des Vosges,
La Défense 5
F-92400 Courbevoie(FR)

(72) Inventor: **Naccache, David**
46, rue St. George
F-94700 Maisons-Alfort(FR)
Inventor: **Fremanteau, Patrice**
30, rue des Carmes
F-67100 Strasbourg(FR)

(74) Representative: **Einsel, Robert, Dipl.-Ing.**
Deutsche Thomson-Brandt GmbH
Patent- und Lizenzabteilung
Göttinger Chaussee 76
D-30453 Hannover (DE)

(54) Unforgeable identification device, identification device reader and method of identification.

(57) Memory cards are cheap and contain memory means, but can be forged and duplicated easily. Smart-cards contain also a micro-processor and can be used for cryptographic purposes, but are much more expensive.
The plastic support (14) of the card contains randomly distributed ferrite particles (11) (eg. small steel marbles, introduced into the plastic paste during the melting process). This random distribution of the particles is assumed to be impossible to control or influence during the process of fabrication. For personalizing a card, the issuing authority scans the plastic support of the card with a magnetic inductance detector, thereby reading the emplacement of the ferrite particles as a number p. Then the authority computes s = SIG(ID,p), where "SIG" denotes any secure public-key digital signature algorithm and ID the identification details of the card's owner. Finally, s and ID are recorded in the memory means (13) of the card. When such a card is inserted into a reader, the reader scans the plastic part of the card and reads the distribution characteristics as a number p. Then ID and s are retrieved from the card's memory means and the reader checks that s is the valid signature of {ID,p}.

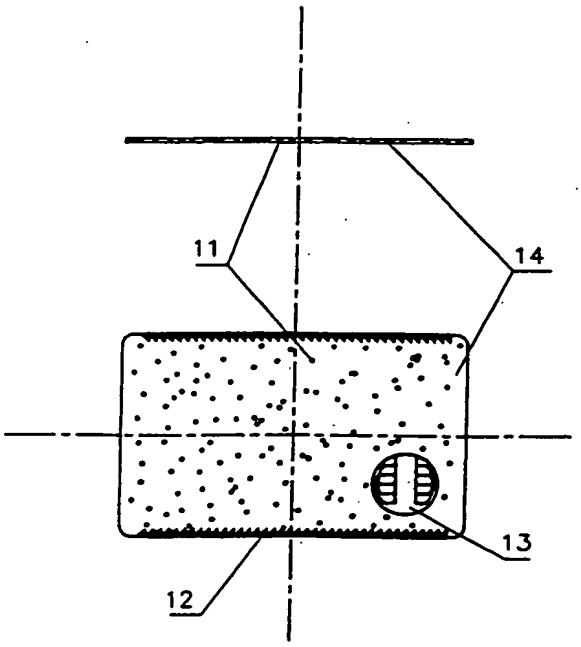

FIG. 1

EP 0 583 709 A1

The present invention relates to an unforgeable identification device, identification device reader and to a method of identification.

Background

Different kind of plastic cards are known. Memory cards are cheap and contain memory means, but can be forged and duplicated easily. Smart-cards contain also a microprocessor and can be used for cryptographic purposes, e.g. in pay TV applications and banking, but are much more expensive.

Invention

It is one object of the invention to disclose a cheap and unforgeable memory card. This object is reached by the identification device disclosed in claim 1.

The inventive memory card is characterized in that once issued by an authority, the card is nearly impossible to copy and duplicate. This new memory card has significant cost advantages over microprocessor-based smart-cards since memory protection means and computation capabilities are no more requested for achieving authentication.
The process of fabrication of the new cards differs from that of standard cards in that small metal or ferrite particles (eg. steel marbles) are mixed with the plastic paste from which the plastic support of the card is to be produced.
Each resulting card will therefore contain a different random distribution pattern of particles. This random distribution of the particles is assumed to be impossible to control or influence during the process of fabrication.
A respective reader is provided with magnetic inductance detectors (reader) that allow to read the distribution of particles as a number p and with a chip reader for reading the card's memory means.
In order to personalize a card, the issuing authority does the following :

1. Establish the identity details ID of the card's owner;
2. Pick a card and read it's random pattern p;
3. Compute s = SIG(ID,p);
4. Record s and ID in the memory means of the card;
5. Give the card to the user.

Here "SIG" stands for any secure public key digital signature scheme. The memory means are preferably electronically protected.

When a memory card is inserted into a verification reader, the reader will scan it and convert the random distribution of particles into the number p. Next, the verification reader will read s and ID from the card's memory means and will check that s is actually the signature of {ID,p} by performing SIG^{-1}.

In principle the inventive unforgeable identification device includes memory means and an area in which elements, the location of which is detectable, have a random distribution which can be represented by a value p, whereby the location of said elements cannot be controlled under production of said device but can be detected and evaluated in reader means and whereby at least identity data ID and data s of a public-key digital signature scheme s = SIG(ID, p) are stored in said memory means.

Advantageous additional embodiments of the inventive identification device are resulting from the respective dependent claims.

It is a further object of the invention to disclose a reader for this identification device. This object is reached by the identification device reader disclosed in claim 6.

In principle the inventive identification device reader includes detector means - especially a magnetic inductance reader - for the location of said elements from which said distribution value p is generated and reading means for at least said identity data ID and data s stored in said memory means of said identification device.

Advantageous additional embodiments of the inventive identification device reader are resulting from the respective dependent claims.

A respective identification system is disclosed in claim 9.

It is a further object of the invention to disclose a method of identification which utilizes the inventive identification device and reader. This object is reached by the method disclosed in claim 10.

In principle the inventive method uses the identification device and the identification device reader and includes the following issuing steps:

- collecting identity details ID of a user;
- computing s = SIG(ID, p), where SIG is a public-key digital signature scheme function;
- storing s and ID in said memory means of said identification device,

and includes the following identification steps:

- reading said identification device by said identification device reader, whereby said distribution value p is generated and at least s and ID are read from said memory means;
- checking that s is actually the signature of (ID, p) by performing the respective inverse public-key digital signature scheme function SIG^{-1}.

Advantageous additional embodiments of the inventive method are resulting from the respective dependent claims.

Drawings

Preferred embodiments of the invention are described with reference to the accompanying drawings, which show in:

Fig. 1 structure of an inventive memory card;

Fig. 2 structure of an inventive reader for the memory card.

Preferred embodiments

In Fig. 1 buried ferrite particles 11 are distributed within the plastic support 14 of a memory card with standardized shape. This card contains a chip 13 with which data can be exchanged in a respective reader, e.g. contactless. At two sides of the card electronic scanner synchronisation marks 12 are arranged.

In Fig. 2 the card is inserted in a reader (scanner). The reader includes electromagnetic scanning cells 22 for generating the distribution value p, e.g. an optical scanning synchronization head 23 and reading means (smart-card chip reader) 24 for at least the identity data ID and data s stored in the memory of the chip 13. ID, s, the distribution value p and possibly the password w are evaluated in a microprocessor 21 which can be a part of the reader device.

One example of digital signature schemes is Rabin's signature scheme where n is an RSA modulus and s is defined by $s = SIG(m) = m^{1/2} \bmod n$. The corresponding verification is done by checking that $s^2 \bmod n = m$.

Optionally, one can improve the basic scheme by including also a user's password w. In such a case, the process of issuing a card and verifying it's validity becomes :

1. Establish the identity details ID of the card's owner.
2. Pick a card and read it's random pattern p.
3. Decide about a password w specific to the user.
4. Compute s = SIG(ID,p,w)
5. Record s and ID in the memory means of the card.
6. Give the card and w to the user.

For verifying the validity of this card, the verification reader will proceed as before but will request from the user to key-in w.

The SIG scheme can be one of the following or respective methods:

- Rabin's digital signature;
- RSA algorithm, Rivest, Shamir, Adelman, "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, Vol 21, No 2, pp 120-126, 1978);
- Data Signature Standard (DSS);
- El Gamal, "A public-key cryptosystem and a signature scheme based on the discrete logarithm", IEEE Transactions on Information Theory, vol. 31, No. 4, pp. 469-472, 1985;
- Fiat, Feige and Shamir, "Zero-Knowledge Proofs of Identity", Journal of Cryptology, vol 1, pp. 77-94. See also EP-A-0252499 and EP-A-0325238.

For synchronizing the scanning of the ferrite particles (whatever the insertion speed of the card is), the card can be marked, e.g. at the boundaries, by a sequence of mechanical (embossed or holes) or optical marks. The marks are preferably detected optically by the reader and trigger the scanning of plastic band by band. The marks can also be based on electromagnetic detection techniques and the triggering of the scanning is done accordingly.

Instead of plastic material any other material can be taken which allows detection of the distribution of the particles. Instead of magnetic particles also other kind of elements can be taken, the distribution of which can be detected and which do not allow copying.

Instead of a card any other kind of device or shape can be used, whereby the reader is adapted respectively.

Identification shall also mean authentication.

Claims

1. Unforgeable identification device, including memory means (in 13) and an area (14) in which elements (11), the location of which is detectable, have a random distribution which can be represented by a value p, whereby the location of said elements cannot be controlled under production of said device but can be detected and evaluated in reader means (22) and whereby at least identity data ID and data s of a public-key digital signature scheme s = SIG(ID, p) are stored in said memory means.

2. Device according to claim 1, **characterized in** that said area (14) is made from plastic material in which magnetic particles (11) - especially steel or ferrite pellets - are contained.

3. Device according to claim 1 or 2, **characterized in** that said memory means (in 13) are of type electronic unprotected or protected.

4. Device according to any of claims 1 to 3, **characterized in** that said device is marked (12) for scanning control, e.g. scanning speed and/or synchronisation.

5. Device according to any of claims 1 to 4, **characterized in** that said device is a standardized memory card.

6. Identification device reader for an identification device according to any of claims 1 to 5, including detector means (22) - especially a magnetic inductance reader - for the location of said elements (11) from which said distribution value p is generated and reading means (24) for at least said identity data ID and data s stored in said memory means (in 13) of said identification device.

7. Reader according to claim 6, including means (23) for evaluating said scanning control marks (12).

8. Reader according to claim 6 or 7, including computing means (21) for evaluating at least ID, s and p.

9. Identification system, including an identification device according to any of claims 1 to 5 and an identification device reader according to any of claims 6 to 8.

10. Method of identification, which uses an identification device according to any of claims 1 to 5 and an identification device reader according to any of claims 6 to 8, including the following issuing steps:
    - collecting identity details ID of a user;
    - computing s = SIG(ID, p), where SIG is a public-key digital signature scheme function;
    - storing s and ID in said memory means (in 13) of said identification device,

    and including the following identification steps:
    - reading said identification device by said identification device reader, whereby said distribution value p is generated (22) and at least s and ID are read from said memory means (in 13);
    - checking that s is actually the signature of ID and p concatenated by performing (21) the respective inverse public-key digital signature scheme function SIG^{-1}.

11. Method according to claim 10, **characterized in** that in the issuing steps said public-key digital signature scheme s = SIG(ID, p, w) includes a password w specific to said user and that in the identification steps the user enters said password w, whereafter it is checked that s is actually the signature of ID, p and w concatenated.

12. Method according to claim 10 or 11, **characterized in** that said reading of said identification device is synchronised using said scanning control marks (12).

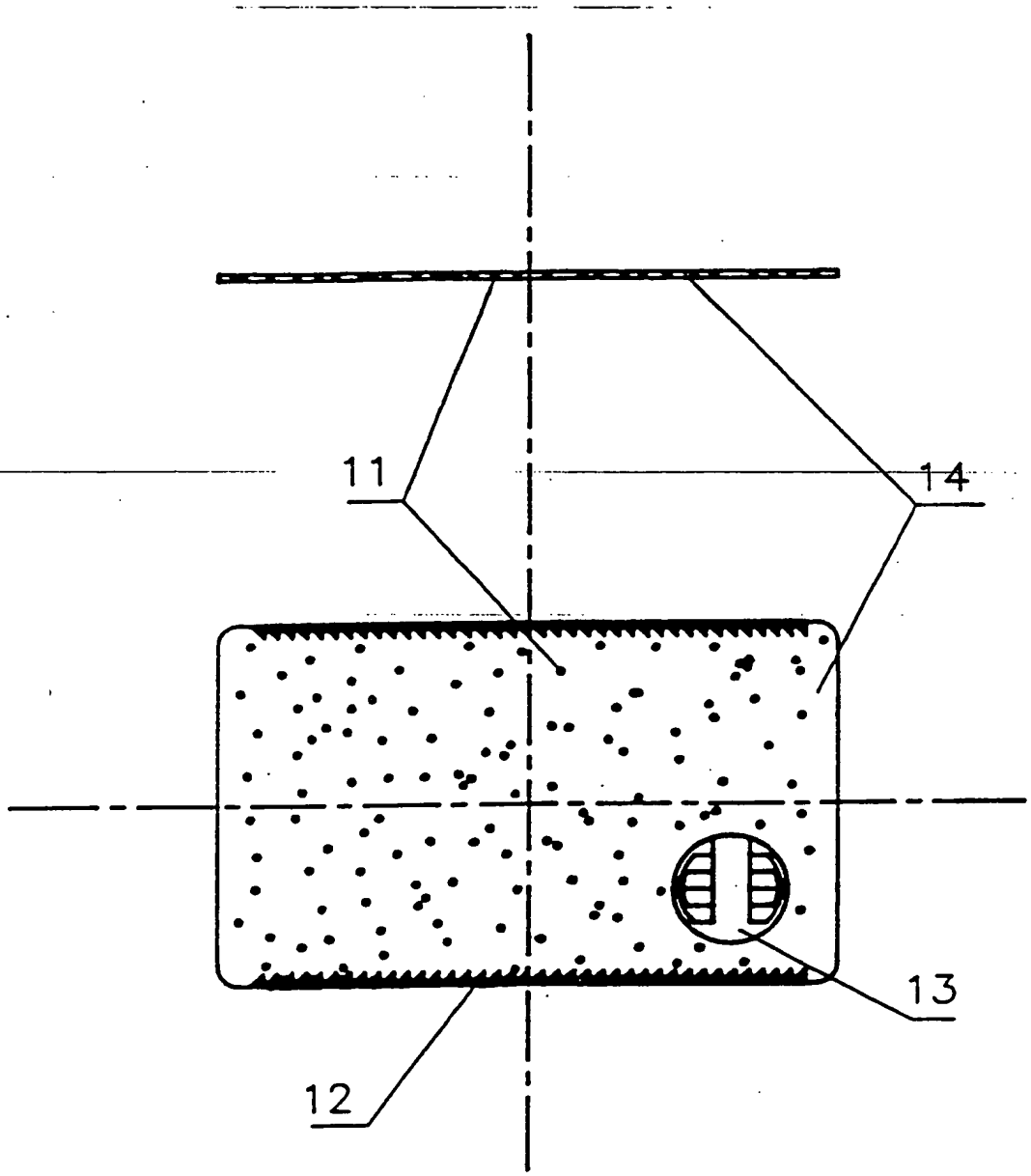

FIG. 1

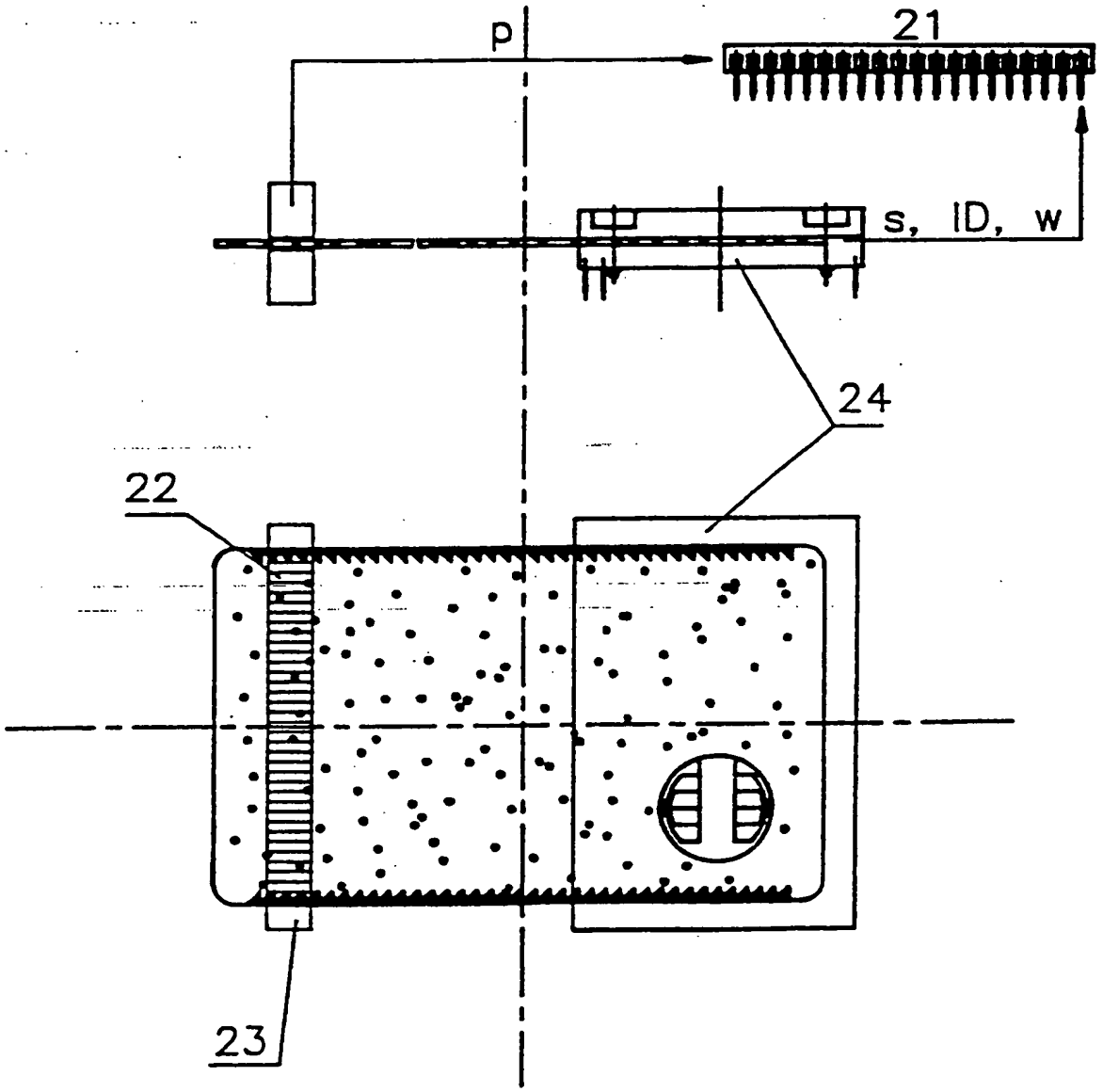

FIG. 2

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 93 11 2678

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int. Cl.5)
Y	EP-A-0 298 156 (LIGHT SIGNATURES, INC.)	1,2,4-7, 10,12	G06K19/10 G07F7/08
A	* column 3, line 55 - column 4, line 9; figure 1 * * column 5, line 26 - line 43 *	8,9,11	
Y	US-A-4 094 462 (MOSCHNER) * abstract; figure 1 * * column 2, line 1 - line 25 *	1,2,4-7, 10,12	
A	US-A-4 527 051 (STENZEL) * abstract; figure 1 * * column 8, line 5 - line 15 *	2	
A	EP-A-0 161 181 (SOCIÉTÉ D'ÉLECTRONIQUE DE LA RÉGION PAYS DE LOIRE-SEREL) * abstract; claim 1; figure 1 *	1,5,6, 8-10	
A	EP-A-0 451 024 (GEMPLUS CARD INTERNATIONAL) * the whole document *	3	TECHNICAL FIELDS SEARCHED (Int. Cl.5)
D,A	EP-A-0 252 499 (YEDA RESEARCH AND DEVELOPMENT COMPANY, LIMITED) * the whole document *	1,9,10	G06K G07F

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	17 SEPTEMBER 1993	CHIARIZIA S.J.

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P0601)